

EXHIBIT 61

Message

From: Nick Salsman (Basecamp) [notifications@3.basecamp.com]
Sent: 8/14/2020 8:45:33 PM
To: Hamilton, Dave [/o=SOS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1f184986d45c4fc1be9d3ea7a3bb068c-Hamilton, Dave]
Subject: (Elections Center- Infrastructure Server) Proposed changes

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

MicroSemi NTP server racked but powered off – comment made that the “private” domain is off an hour – sometimes two : (must wreak havoc with apps and SQL

NTP device is now functional

- Access to environment is simple username and password – no MFA – strongly recommended – however finesse in implementation due to it’s isolation requirement

RSA tokens have been ordered and received to be able to facilitate 2FA when ready.

- Legacy 1998 Application – Gems – now defunct. Now supported by Dominion

Will stay in place

- New “Democracy Suite” – Dominion – Windows 10 based client, unsure about supporting backend requirements other than SQL Server 2005?? – confirm version build level

Supports SQL Express in Win10 client config, this planned config. SQL Express installs per Win10 VM.

- Windows 10 running XP guest to access old system.

Will continue to be able to provide legacy needs until further notice

- Server Host – VMWare 5.5 – all on private

New server host is ESXi 6.0 U3, max version supported by server hardware due to age

- No history of patching anything

New server is on the maximum supported build of ESXi and firmware of host.

- Need to trace, label and identify private station cables – Has Cisco L3 capabilities to provide NAC protection – or just disconnect at the patch panel to prevent inadvertent connections to private by unknown clients

Threat will be mitigated by introducing a Cisco 24 port switch which then feeds into a Palo Alto 820 Firewall. Users will have to VPN through the FW to gain access to servers.

- Need to be able to scan every USB attached storage device connected prior to use. Cannot ensure USB is free from malware, keylogging, etc. Should not impose a unreasonable delay in use to impact workflow.

We're proposing the use of DataLocker secure USB drives. This will give us phone home capabilities along with live AV scanning built in.



You can reply to this email or [respond in Basecamp](#).

This message was sent to Dave Hamilton, KRobertson, Nick Salsman, Ronnell Spearman, and Terrence Reese.

[Unsubscribe](#) • [Change your notification settings](#)

Get the Basecamp app for iPhone or Android!

